

Using DLSw+ with Other Features

This chapter describes how to use DLSw+ in conjunction with other Cisco IOS Software features: SNA Switching Services (SNASw), DSPU, NCIA, and LAN Network Manager. It briefly describes these features, discusses why you would want to run these features in the same router with DLSw+, and provides some sample configurations.

Using DLSw+ with SNASw

DLSw+ TCP encapsulation supports SNASw, Cisco's second-generation APPN platform in Cisco IOS Release 12.1 and higher (DLSw+ FST does not support SNASw). SNASw, available in Cisco IOS Release 12.1 and later, replaces the function provided by the APPN network node (NN) feature of Cisco IOS Software. Cisco is discontinuing the APPN NN feature in Cisco IOS Software beginning with Release 12.1 because of its architectural complexity, scaling limitations, and manageability issues. Older versions of Cisco IOS Software prior to Release 12.1 are reaching their end of engineering support as follows:

- *Release 11.2*—April 16, 2001
- *Release 12.0*—After March 2002

This section discusses why and where SNASw is required, explains the circumstances in which you would run SNASw and DLSw+ together in the same router, and provides an example of how to configure it. SNASw and DLSw+ positioning and interoperability are extensively covered in the *SNASw Design and Implementation Guide* at www.cisco.com/warp/public/cc/pd/ibsw/snasw/tech/snasw_rg.pdf.

What Is APPN?

APPN is an SNA architecture that defines how peer nodes communicate. It differs from subarea SNA in several ways:

- APPN does not have a hierarchical structure; there is no concept of upstream or downstream resources, primary or secondary roles are negotiated, and all network nodes have control points.
- End systems understand the network architecture and are not on the periphery or boundary of SNA; therefore, SNA COS extends to the desktop, and best paths through the network can be determined directly from the end systems.
- APPN is more dynamic; both directory and topology information is determined dynamically with minimal configuration requirements.
- With High Performance Routing (HPR), APPN can dynamically reroute around link failures without disrupting SNA sessions.
- APPN Enterprise Extender (EE) can enable SNA transport over native IP between mainframe hosts (using APPN Extended Border Node) or host-to-peripheral SNA devices (using SNASw EE support).

Where and Why to Use SNASw with DLSw+

When the IBM APPN architecture was first defined in the mid-1980s, it supported only LU 6.2 applications. Because most applications were subarea SNA 3270 applications, there was limited migration toward APPN in corporate networks. In VTAM V4R2, however, VTAM implemented a feature known as Dependent LU Server (DLUS). When used in conjunction with Dependent LU Requester (DLUR), this feature allows you to use APPN for any SNA application in your network.

SNASw provides DLUR support, which allows SNASw to connect to an upstream DLUS server on a NN server host. This provides dependent PU 2.0 support for peripheral SNA devices.

Where SNASw is implemented depends on the problem you are trying to address. It can be implemented in the data center, distribution layer, or branch.

SNASw in the Data Center

In multihost environments and hosts with multiple logical partitions (LPARs), SNASw allows you to reduce costs and enhance performance by minimizing your dependency on FEPs and NCP software, while migrating to a Cisco CIP/CPA or Catalyst 6500 switch Gigabit Ethernet-attached to an IBM Open Systems Adapter-Express (OSA-Express) on an IBM S/390 or zSeries host.

SNASw and HPR in the data center also allow you to enhance SNA application availability by taking advantage of the capabilities of an IBM Parallel Sysplex (which requires APPN and HPR). This implementation provides the functions required to support necessary SNA routing of client sessions directly to the target application host in addition to providing DLSw+ peer termination points for WAN transport of SNA from remote SNA clients.

By running DLSw+ in the same router as SNASw, you can use the existing DLSw+ network to transport SNA traffic from remote sites over the WAN to the data center and use Cisco's SNASw implementation in the data center to handle SNA routing of client sessions directly to the correct SNA application host, handle DLUR processing for dependent SNA devices, and provide EE support to natively transport the SNA traffic over IP into the IBM S/390 or zSeries host.

SNASw in the Distribution Layer

SNASw can reduce FEP requirements at regional distribution sites while maintaining SNA routing functionality. In multiple data center environments, you can use Cisco routers with SNASw functionality where you have FEPs today to support SNA application routing and preserve COS. Cisco routers cost considerably less than FEPs, are much easier to maintain, support more diverse LAN and WAN media, and can be used to support multiprotocol traffic such as voice over IP (VoIP) and multimedia. By limiting SNASw to the distribution layer and utilizing an existing DLSw+ for remote SNA transport over the WAN, you can minimize cost and avoid scalability issues while still getting the benefit of routing SNA client sessions directly to the target data center application host.

SNASw to the Branch

SNASw can be also deployed to the remote branch. In this case, SNASw can support SNA transport over native IP without any requirement to use DLSw+ for SNA WAN transport. This is accomplished using the SNASw EE feature. Additional details regarding this feature can be found in the *SNASw Design and Implementation Guide* at www.cisco.com/warp/public/cc/pd/ibsw/snasw/tech/snasw_rg.pdf.

VDLC Transport

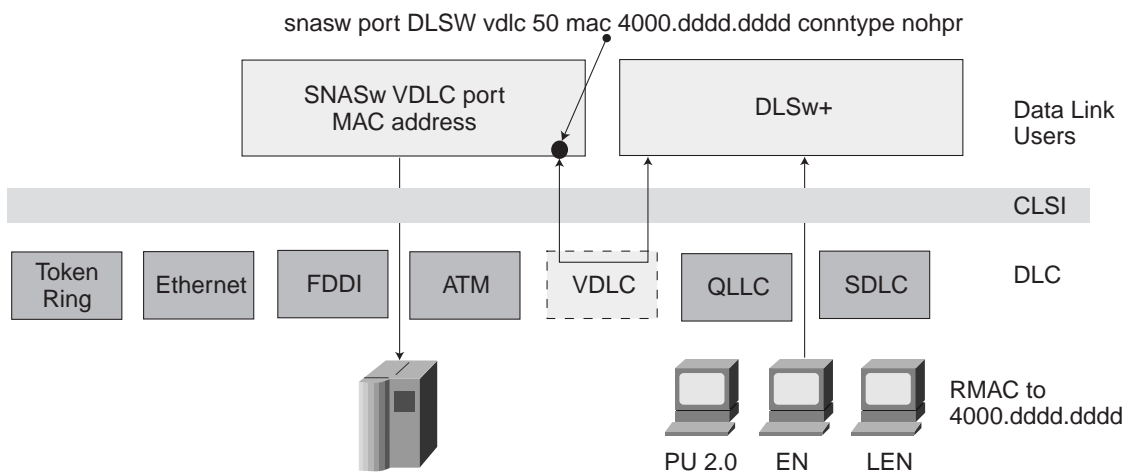
SNASw uses Virtual Data Link Control (VDLC) to connect to DLSw+ transport and local switching technologies. VDLC is used for a number of connectivity options, including:

- Transport over DLSw+ supported media
- DLC local switching support for access to SDLC and QLLC

Using VDLC, SNASw gains full access to DLSw+ SNA transport capabilities, including DLSw+ transport over IP networks, DLSw+ transport over direct interfaces, and DLSw+ support of direct Frame Relay encapsulation (without using IP). SNASw also gains access to devices connecting through SDLC and QLLC (see Figure 11-1).

Note: SDLC and QLLC are transparent to the SNASw code.

Figure 11-1 VDLC Transport



Configuration Details

To configure DLSw+ and SNASw interoperability you need to do the following:

- Configure DLSw+ TCP encapsulation (DLSw+ FST does not interoperate with SNASw because FST does not support VDLC)
- Configure the SNASw control point
- Configure SNASw to transport data over VDLC and define its virtual MAC address
- Configure SNASw links to the upstream NN server host and backup NN server
- Configure SNASw connection network to support dynamic links to all other upstream application hosts

Note: For additional information on SNASw DLSw+ configuration, see the *SNASw Design and Implementation Guide* and the following documentation:

- *Cisco IOS Bridging and IBM Networking Configuration Guide*, Release 12.1, “Configuring SNA Switching Services” (Cisco Documentation CD-ROM or www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/ibm_c/bcprt2/bcdsnasw.htm)
- *Cisco IOS Bridging and IBM Networking Configuration Guide*, Release 12.1, “SNA Switching Services Commands” (Cisco Documentation CD-ROM or www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/ibm_r2/br2prt1/br2dsnaw.htm)

The following sample illustrates SNASw DLSw+ configuration (using DLSw+ local switching):

```
source-bridge ring-group 1072
dlsw local-peer
!

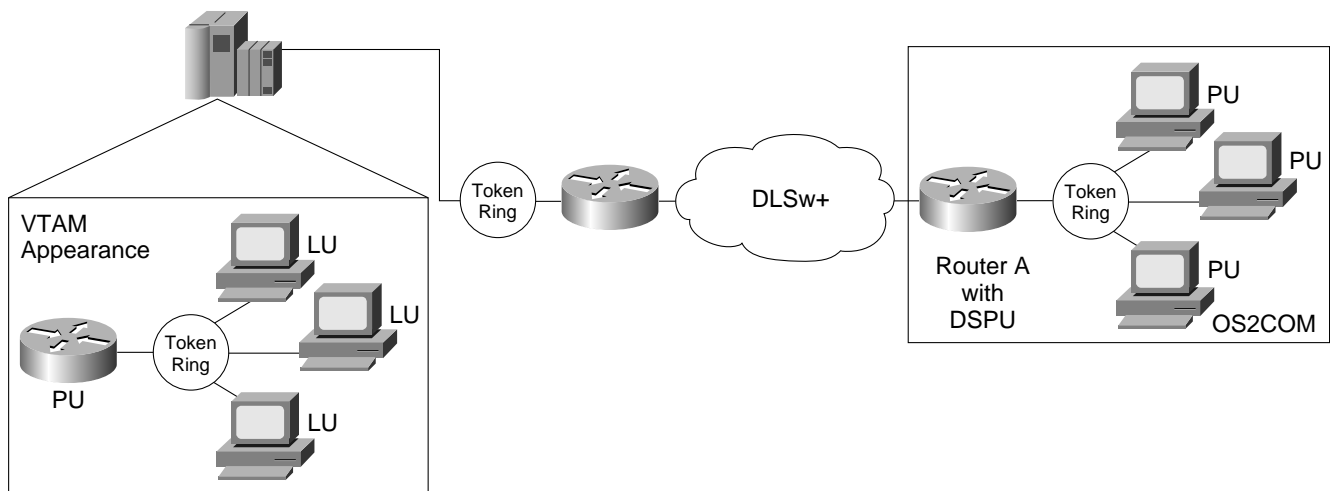
interface Serial0/1
 no ip address
 encapsulation sdhc
 no keepalive
 nrzi-encoding
 clockrate 9600
 sdhc role primary
 sdhc vmac 4000.3174.0000
 sdhc address C5
 sdhc xid C5 01722222
 sdhc partner 4000.4500.00f0 C5
 sdhc line-speed 9600
 sdhc dlsw C5
!

snasw cpname NETA.R6072
snasw port DLSWPORT vdlc 1072 mac 4000.4500.00f0
snasw port SER0 hpr-ip Serial0/0
snasw link BMVS port SER0 ip-dest 192.168.237.129
```

Using DLSw+ with DSPU

DSPU is an old Cisco IOS IBM feature that historically has been used for consolidating multiple remote SNA 3270 workstations (running 3270 emulation software) or 3270 controllers with minimal SNA LU per PU requirements into a single upstream host (VTAM) PU appearance (see Figure 11-2). DSPU can consolidate devices up to the 255 SNA LU per PU IBM SSCP architectural limitation. In situations where a remote branch office has 20 to 30 (or more) PCs running 3270 emulation software, this could amount to a very large number of SNA PU resources that would need to be configured, enabled, and supported on the enterprise host (CS/390).

Figure 11-2 DSPU Concentrates SNA PUs



If a customer, for example, had 300 remote branch offices, this could equate to as many as 6000 to 9000 PUs in the network that would need to be configured in the host. In this case, DSPU could potentially reduce the CS/390 SNA PU configuration requirement to 300 PUs if each remote branch office had a total SNA LU requirement of 255 LUs per branch.

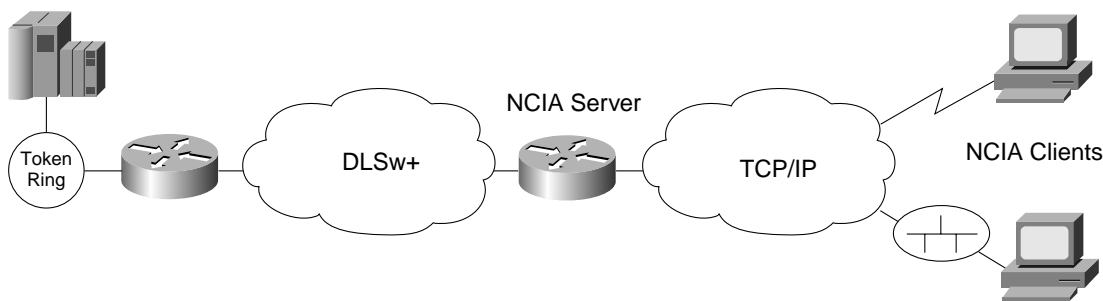
The maximum number of DSPU PUs that can be configured on a single DSPU router is 4096 in the latest versions of the Cisco IOS Software (Release 12.1 and higher).

There are many other Cisco IOS IBM features that can better be utilized to support SNA LU 2.0 green screen and 3270 emulation requirements (CIP/CPA TN3270 Server and SNASw DLUR support).

Using DLSw+ with NCIA

NCIA Server is an old Cisco IOS feature that connects NCIA clients over TCP/IP. The connection from the router running NCIA Server back to the data center host can utilize DLSw+ SNA WAN transport upstream. Figure 11-3 illustrates how NCIA interoperates with DLSw+.

Figure 11-3 NCIA Server Used with DLSw+



The NCIA Phase II architecture (RFC 2114) was originally developed by Cisco several years ago and submitted to the Internet Engineering Task Force (IETF) to address early customer requirements for SNA application access over IP backbone (the IETF specification refers to the architecture as the DLSw Remote Access Protocol [DRAP]).

TN3270 Server (supported on the CIP and CPA) provides similar functions to NCIA. Both allow client emulator software packages access to existing IBM mainframe applications, and both support TCP/IP as the backbone transport for these sessions. However, NCIA differs from TN3270 Server in that with NCIA, the client actually runs a full SNA emulator, as opposed to TN3270 Server where the client needs to run only TN3270 client software.

With NCIA, the client is a full SNA PU and LU. With TN3270, the SNA PU and LUs are located on the TN3270 Server. In both NCIA and TN3270 Server, the native protocol from the client PC is TCP/IP. The primary difference between these implementations is in the location of the SNA PUs and LUs. The NCIA approach is that the full SNA capability built into the SNA 3270 emulator itself is maintained.

The primary advantage of the TN3270 Server approach is that the definition and configuration are eased because each client looks like one or more LUs but does not require the definition of a PU. TN3270 Server is also an accepted industry standard with a very large installed base of devices supporting it (NCIA, on the other hand, is a technology on the way to being phased out).

Cisco DLSw+ does interoperate with NCIA Server Phase I.

Using DLSw+ with LAN Network Manager

IBM's LAN Network Manager is a management tool used to manage Token Ring media attachment units (MAUs) and Token Ring adapters. It uses a proprietary protocol to communicate with agent software in source-route bridges and in Cisco routers to obtain the status of the Token Ring network and to send commands to Token Ring-attached devices.

When using DLSw+ with LAN Network Manager, your LAN Network Manager displays will be more meaningful if you use the same virtual ring number everywhere. There are no special configuration requirements to use LAN Network Manager in conjunction with DLSw+.